

MONTGOMERY -- 09/823,278
Client/Matter: 042503-0261929

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of producing a stream of digital data comprising the step of:

determining a plurality of portions within the stream of digital data, such that a portion of the stream of digital data is encrypted with an encryption key that is capable of being decrypted by a decryption key and the portion including therein another decryption key capable of decrypting a subsequent portion of the stream of digital data wherein data identifying the location of the another decryption key is in a location other than as part of the encryption key, and

the subsequent portion of the stream of digital data is encrypted with another encryption key that is capable of being decrypted by the another decryption key; and

transmitting the stream of digital data, including the portion and the subsequent portion.

2. (Original) A method according to claim 1 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is included therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data.

3. (Original) A method according to claim 2 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.

4. (Original) A method according to claim 3 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

5. (Original) A method according to claim 3 wherein the encryption key and decryption key certain ones of the another encryption keys and another decryption keys have a different key length.

MONTGOMERY -- 09/823,278
 Client/Matter: 042503-0261929

6. (Original) A method according to claim 2 wherein the decryption key and each another decryption key is located at a different location within each portion.
7. (Original) A method according to claim 2 wherein each portion has a different bit size.
8. (Original) A method according to claim 2 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
9. (Original) A method according to claim 8 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.
10. (Original) A method according to claim 9 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.
11. (Original) A method according to claim 2 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.
12. (Original) A method according to claim 11 wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.
13. (Original) A method according to claim 1 wherein the another decryption key is encrypted with the encryption key.
14. (Original) A method according to claim 13 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
15. (Original) A method according to claim 13 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.
16. (Original) A method according to claim 14 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

MONTGOMERY - 09/823,278
Client/Matter: 042503-0261929

17. (Original) A method according to claim 16 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

18. (Original) A method according to claim 17 wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

19. (Original) A method according to claim 1 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.

20. (Original) A method according to claim 19 wherein the marker and the another decryption key is encrypted with the encryption key.

21. (Original) A method according to claim 20 wherein each encryption key is different and each decryption key is correspondingly different.

22. (Original) A method according to claim 21 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.

23. (Original) A method according to claim 22 wherein each portion has a different size.

24. (Original) A method according to claim 22 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

25. (Original) A method according to claim 19 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

26. (Original) A method according to claim 1 further including, prior to the step of transmitting the stream of digital data, the steps of:

transmitting a decryption key that is capable of decrypting the portion of the stream of digital data; and

receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data.

27. (Original) A method according to claim 1 further including, prior to step of transmitting the stream of digital data, the steps of:

MONTGOMERY -- 09/823,278
 Client/Matter: 042503-0261929

transmitting a set-up stream including an encrypted test decoder and an encrypted and encoded test sequence; and

receiving an acknowledgement with monitor information indicative of performance of an end-user computer; and

determining a key length and a key rotation period based upon the monitor information.

28. (Original) A method according to claim 27 wherein the monitor information provides an amount of time required to decrypt and install the decryption key and decrypt and decode the test sequence.

29. (Original) A method according to claim 26 wherein, an encrypted executable decoder is included in the portion of the stream of digital data, the encrypted executable decoder, when decrypted and installed, being capable of decoding data content that is also included in the portion of the stream of digital data.

30. (Original) A method according to claim 29 wherein the encrypted executable decoder can be decrypted using the decryption key.

31. (Original) A method according to claim 26 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is including therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data.

32. (Original) A method according to claim 31 wherein

the another decryption key is located within the portion at a location that precedes the end the portion by an amount that will ensure the remaining transmission time of the portion after transmission of the another decryption key is greater than a latency measurement indicating an amount of time required to decrypt and install the decryption key; and

each another decryption key is located within each subsequent portion at another location that precedes the end the subsequent portion by another amount that will ensure the remaining transmission time of that subsequent portion after transmission of the corresponding another decryption key is greater than the latency measurement.

MONTGOMERY - 09/823,278
 Client/Matter: 042503-0261929

33. (Original) A method according to claim 31 wherein each encryption key is different and each decryption key is correspondingly different.

34. (Original) A method according to claim 33 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

35. (Original) A method according to claim 33 wherein the encryption key and decryption key and certain ones of the another encryption keys and another decryption keys have a different key length.

36. (Original) A method according to claim 31 wherein each portion has a different bit size.

37. (Original) A method according to claim 31 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

38. (Original) A method according to claim 31 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

39. (Original) A method according to claim 38 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

40. (Original) A method according to claim 39 wherein the each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

41. (Original) A method according to claim 26 wherein the another decryption key is encrypted with the encryption key.

42. (Original) A method according to claim 26 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.

43. (Original) A method according to claim 42 wherein the marker and the another decryption key is encrypted with the encryption key.

44. (Original) A method according to claim 43 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.

MONTGOMERY -- 09/823,278
Client/Matter: 042503-0261929

45. (Original) A method according to claim 44 wherein each portion has a different bit size.

46. (Original) A method according to claim 42 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

47. (Original) A method according to claim 42 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

48. (Original) A method according to claim 1 wherein:
the portion immediately precedes the subsequent portion; and
the another decryption key is located within the portion at a location that precedes the end of the portion by an amount that will ensure the remaining transmission time of the portion after transmission of the another decryption key is greater than a period of time needed to decrypt and install the another decryption key.

49. (Original) A method according to claim 48 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

69. (Currently Amended) A method of decrypting a stream of digital data comprising the steps of:

receiving a portion of the stream digital data, the first portion being encrypted with an encryption key capable of being decrypted by a decryption key and including a subsequent decryption key capable of decrypting a subsequent portion of the stream of packets of digital data;

decrypting the portion of the stream of digital data using the decryption key;

identifying the subsequent decryption key disposed within the portion of the stream of digital data using location data for the subsequent decryption key prior to completion of decrypting the portion of the stream of digital data, wherein the location data is at a location other than as a portion of the encryption key;

installing the subsequent decryption key data prior to completion of decrypting the portion of the stream of digital data; and

MONTGOMERY -- 09/823,278
 Client/Matter: 042503-0261929

receiving another portion of the stream of packets of digital data, the another portion being encrypted with another encryption key that is capable of being decrypted by the subsequent decryption key; and

decrypting the another portion of the stream of digital data using the subsequent decryption key.

70. (Original) A method according to claim 69 wherein the portion and the another portion each include a plurality of packets, and each of the packets contains a non-encrypted header identifying that the decryption key and the subsequent decryption key, respectively, should be used during the respective step of decrypting.

71. (Original) A method according to claim 70 wherein the step of identifying includes the step of locating a marker that immediately precedes the subsequent decryption key.

72. (Original) A method according to claim 71 wherein the step of installing stores the subsequent decryption key at a memory address location that is different from the decryption key.

73. (Original) A method according to claim 71 further including additional steps of receiving and decrypting the another portion, and for each additional another portion, there is included

a step of identifying each additional subsequent decryption key; and

a step of installing each additional subsequent decryption key, the step of installing including the step of storing each additional subsequent decryption key at a memory address location that is different from the immediately preceding subsequent decryption key.

74. (Original) A method according to claim 73 wherein each memory address location for each additional subsequent decryption key is different.